CORPORATE CONTINGENCY PLANNING

CHAPTER 10

(FILE NAME ON DISK # 1 = S2C10.WPD)

The board of directors and senior management are responsible for establishing policies, procedures, and responsibilities for organization-wide contingency planning. The institution's contingency plan should address all critical services and operations which are provided by internal departments and external sources. The plan should be a coordinated effort with the objectives of minimizing disruptions of service to the institution and its customers, minimizing financial losses, and ensuring a timely resumption of operations in the event of a disaster.

This chapter is divided into two primary sections. The first section will discuss the responsibilities of an institution's board of directors and senior management in providing contingency planning on an organization-wide basis. The second section will discuss a subset of the organization's plan dealing with the resumption of IS operations following a disruption of processing.

CORPORATE CONTINGENCY PLANNING RESPONSIBILITIES

Corporate contingency planning is a process of reviewing an institution's various departments, business units, or functions and assessing each area's importance for the viability of the organization and providing customer services. Plans are then developed to restore critical areas should they be affected by physical disasters, such as fires or flooding; environmental disasters, such as power failure or telecommunication failure; or, other disasters, such as theft or restricted access to facilities.

The board of directors is responsible for annually reviewing and approving the institution's disaster recovery plans. In addition, the board should be apprised of the scope, frequency and test results of the plan's effectiveness. Senior management is charged with conducting a periodic assessment of the criticality of all business areas, evaluating the area's susceptibility to disasters (including their dependence on continued performance by outside parties), and formulating and testing contingency plans. As stated above, one of the primary objectives in corporate contingency planning is limiting financial losses should a disaster occur. A well researched, current, and comprehensive contingency plan will greatly aid management in selecting reasonable cost solutions in highly stressful disaster situations. (See FFIEC Examination Policy SP-5: "Interagency Policy On Contingency Planning For Financial Institutions.")

ORGANIZATIONAL PLANNING GUIDELINES

At a minimum, the board of directors and/or senior management should:

Obtain commitment from senior management to develop the plan.

Establish a management group to oversee development and implementation of the plan. In larger institutions this may involve a full-time staff to coordinate and track individual business unit plans.

Perform a risk assessment.

- Consider possible threats such as:
  - Natural: fires, flood, earthquakes.
  - Technical: hardware/software failure, power disruption, communications interference, etc.
  - Human: riots, strikes, disgruntled employee, sabotage, etc.
- Assess impacts from loss of information and services from both internal and external sources:
  - Financial condition.
  - Competitive position.
  - Customer confidence.
  - Legal/regulatory requirements.

- Analyze costs to minimize exposures.

- Evaluate critical needs. This evaluation also should consider timeframes in which a specific function becomes critical.

  - Functional operations.
  - Key personnel
  - Information
  - Processing systems
  - Documentation
  - Vital records
  - Policies/procedures

- Establish priorities for recovery based on critical needs.

- Determine strategies to recover.

  - Facilities.
  - Hardware.
  - Software.
  - Communications.
  - Data files.
  - Customer services.
  - User operations.
  - MIS.
  - End-user systems.
  - Other processing operations.

- Obtain written backup agreements/contracts for:

  - Facilities.
  - Hardware.
  - Software.
  - Vendors.
  - Suppliers.
  - Disaster recovery services.
  - Reciprocal agreements.

- Organize and document a written plan.

  - Assign responsibilities to:
    - Management.
    - Personnel.
    - Teams.
    - Vendors.
    - Security.

- Document strategies and procedures to recover.

- Develop procedures to execute the plan's priorities for critical vs. non-critical functions:

  - Site relocation (short-term).
  - Site restoration (long-term).
    - Human.
    - Financial.
    - Technical (hardware/software).
  - Data.
  - Facilities.
  - Administrative.
  - Vendor support.

- Establish criteria for testing and maintenance of plans.

- Determine conditions and frequency for testing :

  - Batch systems.
  - On-line systems.
  - Communications networks.
  - User operations.
  - End-user systems.
  - Evaluate results of tests.

- Establish procedures to revise and maintain the plan.

- Provide training for personnel involved in the plan's execution.

- Present the contingency plan to senior management and the board for review and approval.

- After approval, store a copy of the plan off-site with other reserve supplies.

Many materials on contingency/disaster recovery planning have been published by trade associations, accounting firms, and the disaster recovery industry. These can be valuable guides to comprehensive contingency planning.

Reserve supplies should be maintained in appropriate quantities at an off-site location. Management should maintain a current inventory of what is held in the reserve supply.

BACKUP AND CONTINGENCY PLANNING

Disaster recovery planning is a vital to the overall automation security program and the safety and soundness of any institution. The disaster recovery plan should be part of the business resumption plan, which covers every aspect of the bank in the event of an emergency. The ability to efficiently and effectively

recover operations after an emergency reduces the risk of financial loss to the organization and minimizes the level of disruption to the customer.

The disaster recovery plan should not be restricted to traditional mainframe and minicomputer environments. Because of the proliferation of microcomputers and distributed data processing environments (local area networks), critical applications no longer reside only on mainframes or minicomputers. In addition, disaster recovery and contingency planning are not only for large IS operations and facilities, but for institutions with smaller computer systems as well.

The disaster recovery plan should include protection against physical disasters and other disruptions to operations; backup considerations related to hardware, software, applications, documentation, procedures, data files, and telecommunications; and insurance policies regardless of the type of computer equipment and software, and size of the IS facilities within the organization. The contingency plan should be written, approved by the board of directors, and tested annually. This preparation will enhance employee responsiveness, alleviate confusion, and provide for logical decisions during a crisis.

Microcomputer Contingency Planning

The importance of adequate backup resources and procedures for microcomputers cannot be overemphasized. Microcomputer hardware and software technology is ever-changing, and current operations quickly can become outdated. Because of this, contingency planning must begin during the initial acquisition stage and be updated as new hardware and software are acquired.

Protections against equipment failure and data loss should be considered for microcomputers. Because microcomputers are often located outside the protected data processing environment, they are exposed to personnel with insufficient training in their use and exposed to ordinary environmental contaminants. These exposures could cause data loss. The amount and nature of data lost can vary, but an effective backup program, could restore normal operations in an organized and efficient manner.

Basic guidelines for IS backup, contingency planning, and disaster recovery are contained in the following sections. Although these guidelines were developed for larger systems, they also are applicable to microcomputers. This section supplements those guidelines by addressing the risks and exposures specific to the backup of microcomputers and their software and data.

Backup provides continuity of operations. It could be as important in a microcomputer environment as it is in large mainframe centers. Backup standards provide:

- Written backup procedures.
- Maintenance of data file listings, their contents, and locations.
- Hardware, software, and network documentation.
- Minimizing risks involved in the transfer of backup data, whether by electronic link to a mainframe or through the physical transportation of diskettes/tapes to and from the storage site.
- Establishing cross-training programs and levels of responsibility for backup personnel.
- Data integrity, client confidentiality, and the physical security of hardcopy output, media, and hardware.

Depending on the size of the institution and the nature of anticipated risks and exposures, the time spent backing up data is minimal compared with the time and effort that could be necessary to restore it. Files that can be backed up within a short period of time may require days, weeks, or months to recreate from hardcopy records. Therefore, adequate procedures must guide backup operations. They should include:

- Identification of an alternate processing mode, e.g., redundant hardware system located elsewhere; or reciprocal agreement to share compatible hardware with other units within the same institution or in another institution; or backup within the mainframe itself (some institutions enter into agreements with vendors for speedy replacement of software and hardware that has been lost or stolen).

- Off-site storage of software and data.
- Frequency of update and retention cycles of backup software and data.
- Periodic review of software and hardware for compatibility with backup resources.
- Periodic testing of backup for effectiveness in restoring normal operations.
- Guidelines for the labeling, listing, transportation and storage of media.

A coordinator should be assigned to monitor a contingency planning program. Depending on the size of the organization, a user group may be formed to develop and update policies and procedures to assure continued program effectiveness. Further, such a group also could aid the coordinator in implementing and monitoring the program. Membership in this group may include:

- Contingency planning coordinator.
- Microcomputer users at line supervision level.
- Network Administrator.
- Security administrator.
- Internal auditor.

Decisions on application and file backup must be based on how critical the application or files are to the institution's operations. In establishing backup priorities, consideration should be given to all types of information and the potential impact from loss of such data. This includes financial, regulatory, and administrative information, and operating and application software. In assigning backup priority, a risk analysis should be performed that addresses whether:

- The loss of these records would significantly impair the institution's operations.
- The records are being used to manage corporate assets or to make decisions regarding their use.
- Their loss would result in lost revenue.
- Any inaccuracy would result in significant impact on the financial institution, customers, or other departments in the institution.

Frequency of file backup must also depend on the criticality of the application and files. Critical data should be backed up using the "grandfather-father-son" method (see Chapter 13). Backup of operating system software and application programs must be performed whenever they are modified or updated.

Microcomputer software and file backup must not always be kept at an off-site location. Depending on the importance of the information, storage of backup diskettes in another part of the building may be sufficient protection. However, this decision should be based on a risk assessment rather than on ease of access. All backup diskettes should be adequately labeled to identify owner, use, and retention period. The storage location – whether on-site or off-site – should be environmentally controlled and secure, with procedural provisions for restricting physical access to authorized personnel.

IS CONTINGENCY PLANNING

A comprehensive plan should be in place to minimize exposure to all notable threats and risks. This program should emphasize the need for asset protection, security, and controls. The degree of control should be based on an assessment of risk relative to the value of the asset or service. It also should reflect proper concerns for the sensitivity of information. Three major areas that must be reviewed are: physical security; data security; and backup and contingency planning. Physical and data security issues are discussed in Chapter 14. Backup and contingency planning issues will be the focus of this section.

PROTECTION AGAINST PHYSICAL DISASTERS AND OTHER DISRUPTIONS

Physical disasters may be created by man or result from natural phenomena. Regardless of the cause, the best defense against severe loss is effective backup procedures covering equipment, data, operating systems, application software, and documentation.

These provisions enable reconstruction to be accomplished with a nominal amount of confusion and delay. A summary of basic security measures for major physical risks follows.

Fire

Computer center personnel must know what to do in a fire emergency. Instructions should be posted in prominent locations. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed and fire drills should be held periodically. Automatic extinguisher systems include halon, carbon dioxide and water sprinklers. These systems should be the staged type, where the action triggered by a fire detector permits time for operator intervention before it shuts down the power. Computer operations personnel should know how to respond to these automatic extinguishing devices, as well as the location and operation of power and other shut-off valves. Waterproof covers should be located near the equipment in the event that the sprinklers are activated. Hand extinguisher and floor tile pullers should be placed in suitable locations that are easily accessible and vividly marked.

All computer installations should be equipped with heat or smoke detectors. Ideally, these detectors should be located in the ceiling, in exhaust ducts, and under raised flooring. Detectors situated near air conditioning or intake ducts may hinder the build up of smoke to trigger the alarm. The emergency power shutdown should deactivate the air conditioning. Walls, doors, partitions, and floors should be fire-resistant. Also, the building and equipment should be grounded correctly for protection from electrical hazards.

The extent of fire protection required for a data center depends on the degree of risk a financial institution is willing to accept. If the financial institution has major applications on the computer and if appropriate backup facilities are not available, every effort should be made to install the most effective fire extinguishing system. On the other hand, if adequate backup facilities are available or only minor applications, i.e., fixed assets, payroll, securities, are on the system, extensive fire prevention equipment would not be necessary. On-line systems require increased fire protection, since complete backup is more difficult, if not impossible, to obtain.

Flooding

A financial institution should not locate its computer installation in or near a flood plain. If the computer equipment is placed below ground level or a sprinkler system is used, precautions should be taken to limit water damage. If there is a floor above the computer room, the computer room ceiling should be sealed to prevent water seepage.

Sabotage and Riot

Computer center personnel should know how to handle intruders, telephone bomb threats, and other disturbances. Since attacks on computer installations have occurred, their locations should be inconspicuous. Sabotage could be caused by a disgruntled employee. Therefore, personnel policies should require the immediate termination and removal from the premise of any employee considered a threat. Obviously, locked doors, intrusion detection devices, guards, and other controls that restrict physical access are important preventive measures. As for other disasters, procedures should exist to minimize the probability of occurrence and damage, and to effect a full and prompt recovery.

Power Failure

Voltage coming into the computer room is often monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, an alternative power source should be provided. Independent power supply units consist of gas or diesel generators or a battery arrangement that provides electricity for a limited period of time to allow an orderly shutdown of the system. Larger or more complex systems commonly utilize a combination of batteries and auxiliary generator(s) to create an Uninteruptable Power Supply (UPS). The UPS unit enables operations to continue in the event of a power failure or surge.

Housekeeping Rules

Smoking, eating, and drinking in the computer room or when using any computer equipment, such as a microcomputer, should be prohibited. In addition, computer rooms should be kept clean and organized as extraneous supplies and clutter could inhibit the flow of operations or access to emergency exits and controls.

Fraud or Theft

Physical measures to safeguard against loss from fraud or theft are comparable to those outlined for sabotage and riot. Exposure is reduced by restricting access to information that may be altered or misappropriated. Since fraud or theft may be perpetrated easily by insiders, personnel policies should be designed to minimize that possibility. The computer center may be held liable for release of sensitive or confidential information pertaining to its customers; therefore, special procedures to safeguard information are warranted.

Equipment Failure

Equipment failure may result in extended processing delays. Performance of preventive maintenance enhances system reliability and should be extended to all supporting equipment, such as temperature and humidity control systems and alarm or detecting devices.

HARDWARE BACKUP

Hardware backup is the first step in contingency planning. All computer installations must make formal arrangements for alternative processing capability in the event their data center or any portion of the work environment becomes disabled. These plans can take several forms and involve the use of another financial institution, data center, or other installation. In addition, hardware manufacturers and software vendors can be helpful in locating an alternate processing site and in some cases will be able to provide backup equipment under emergency conditions. The more common plans are:

- *In-house* – Many financial institutions operating more than one CPU or local area network (LAN) may be able to provide their own backup for certain critical applications. If the processors are in separate geographic locations, capable of processing critical applications, and are fully compatible, there may be no for other backup locations. If the processors are both located in the same building, the financial institution must develop a plan for outside backup in the event of emergencies.

- *Service bureau* – Many independent service bureaus can provide financial institutions with backup for critical applications. These installations may charge an annual retainer fee in addition to the normal cost of actual backup processing. They should be able to accept the financial institution's work on short notice.

- *Reciprocal agreement* – Many financial institutions enter into agreements with other financial institutions or data processing centers to provide equipment backup. This arrangement is usually made on a best efforts basis, whereby financial institution A promises to backup financial institution B as long as financial institution A has time available.

- *Recovery operations center (ROC) or hot-site* – There are basically two types of processing backup locations: one without equipment but with power, air conditioning, etc. (shell or cold-site);and another in which compatible computer equipment has been installed and awaits use (hot-site). The ROC with installed equipment is normally used by non-priority customers on a timeshareing or random basis. These customers have agreed in advance to relinquish their use to that of an ROC member that has suffered a disaster.

Forms of ROCs or hot-sites vary. Some IS installations have established their own alternative site, while others have formed a cooperative or joint venture with nearby servicers. Cost is a major factor. Various companies have recently begun to market memberships in ROCs/hot-sites at reasonable annual fees, often constructing the facility after a predetermined number of members have committed to join. They may be either shells or fully operational sites whose economies are gained by sharing the costs. Generally, administrative assistance and priority planning are determined by the ROC vendor, with the major disadvantage being the substantial fee assessed if the facility is used.

Potential misunderstandings may be avoided if the financial institution signs a formal written agreement with the management of the backup site, which specifically identifies the conditions under which the site may be used. Basic concerns in establishing hardware backup arrangements include whether:

- The backup system is physically compatible with the primary system. Both hardware and software must be physically compatible to the primary system to process the financial institution's applications.

- The backup installation is a reasonable distance away from the primary system. Ideally, the backup installation should be far enough away to be on a different electric power grid or free from the same natural disaster (earthquake, hurricane, etc.), but close enough to be reached quickly.

- The backup installation is working at peak load. It is of little value to have a backup site that is easily accessible, but has little or no available computer time.

- The backup installation will be advised of impending changes which may effect compatibility or the ability to provide backup. Location and availability of compatible hardware must also be considered before switching to a new hardware system.

Written contingency procedures should, at a minimum, address:

- Conditions or situations that necessitate using the backup site.

- Responsibility for making a decision and guidelines as to when it should be made.

- Employee and vendor notification.

- Backup site notification.

- Steps to be followed at the backup site.

- Files, input work, special forms, etc., to be taken to the backup site and means of transportation.

The backup site should be tested at least annually and when equipment is changed to ensure continued compatibility. To the extent practicable, operating procedures at the backup site should be established with a level of security protection comparable to that for the main data center and other IS operations outside it.

If the institution is small, it may be possible to revert to manual processing, but only as a final alternative. Skills necessary to operate a manual system are soon lost after the application is automated. Unless those skills are maintained through periodic testing, manual processing is usually not a viable alternative.

Hardware backup procedures in a distributed data processing environment (local area network) are similar to that of a mainframe. In the event of a major problem or catastrophic breakdown, off-site processing capabilities should be arranged to ensure continual operations. Contingency plans should be arranged with another institution, data processing center, or other facility.

A major difference in on-site backup between a LAN and mainframe is fault tolerance which is the ability of the LAN to continue functioning in the event of a breakdown with no damage to data and with no perceptible change in operation. Fault tolerance in a network environment entails a duplicate piece of hardware that automatically takes over in case a component on the primary LAN fails. Fault tolerance in a mainframe environment may be difficult to accomplish since the costs incurred with acquiring additional mainframe equipment may be extensive.

The most widely used method of fault tolerance is disk mirroring and/or disk duplexing. With disk mirroring, all programs and data are backed up in real time to a secondary disk drive that can take over if the primary disk fails. This would allow the first or primary drive to be replaced without disrupting server operations. Disk duplexing can be synonymous with disk mirroring, but disk duplexing generally utilizes two controller cards versus one. Regardless of the exact interpretation, disk duplexing entails a greater degree of redundancy than mirroring.

PROGRAM AND SOFTWARE BACKUP

In addition to hardware backup, program backup is another important phase of contingency planning. Program backup for all hardware platforms consists of three basic areas: operating system software, application software, and documentation. All software and related documentation must have adequate off-premise storage. Even when using a standard software package from one vendor, the software probably will vary from one location to another. Differences may include interest rate modifications, reporting options, account applications, or other options chosen by the institution during or subsequent to system implementation. The more nonstandard an institution's software, the more critical it becomes to have off-site storage.

The operating system software must be backed up with at least two copies of the current version. Without it, even the most sophisticated computer hardware is useless. One copy should be stored in the tape and disk

library for immediate availability in the event the original is impaired; the other copy should be stored in a secure, off-premise location. Duplicate copies should be tested periodically and recreated whenever there is a change to the original.

Application software, which includes both source and object versions of all application programs, must be maintained in the same manner as the operating system software. Backup copies of the programs must be updated as program changes are made. Minor updates to backup copies can be made on a group basis, but major revisions or enhancements to application programs should be updated immediately. Storing, testing, and updating such software should be addressed in the installation's contingency plan.

Software vendors can usually supply institutions with copies of standard application software products if they are destroyed. However, even assuming that the vendor has accurately maintained the institution's parameter selections and modifications, there will probably be additional expenses and some delay in making the software operational. Under these circumstances, the institution is placing responsibility for storing software with vendors. Most vendors are reluctant to guarantee software availability, because they may not have current sets of the institution's software. This does not apply to software kept by third parties under an escrow agreement (See Chapter 12). Thus, a financial institution should maintain its own software backup at an off-site location to be assured of only a limited interruption in processing during an emergency.

Documentation for the operating system and the application programs also should be backed up. A minimum level of documentation should be maintained at an off-site location. This includes current copies of:

- Operating system options and modifications.
- Application flowcharts.
- Descriptive narrative for all systems and programs.
- File layouts and transaction codes.
- Operator run instructions.
- User manuals.

The requirement for off-site storage of user manuals can be satisfied by distributing these documents to user departments remote to the data center and institution.

Procedure manuals also are necessary during disaster recovery. Duplicate copies of all IS related procedures should be stored at the off-site location. These include manuals on systems and programming standards, documentation, file libraries, computer operations procedures, and data control procedures. Most important, a copy of the procedures outlining plans for IS operations during emergencies should be maintained off-premise.

DATA FILE BACKUP

The most important area of backup involves the institution's data files, regardless of the platform in which the data is located. Financial institutions must always be able to generate a current master file. Data files must be backed up both on-site and off-site to provide a recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so that processing can continue in the event of a disaster. The creation and rotation of data file backups is a daily activity in most institutions.

TELECOMMUNICATIONS BACKUP

A data center must develop an effective backup plan that includes an agreement for alternative site processing. For telecommunications, that plan also must address the communications media and equipment. The contingency plan should establish priorities, i.e., bank tellers versus ATMs, data versus voice lines, particular offices or sites, and transactions processed versus inquiries, and should identify critical components of the network (such as if all lines in the building connect to a Private Branch Exchange (PBX) and the building is serviced by a single cable to the telephone company central office (CO), alternate routes to the backup CO must be identified as well). Rerouting and redundancy may permit the use of alternate equipment, facilities, lines and circuits, but may still be limited by other considerations. Considerations include risk versus economics, the practicality of the selected backup components, and the security and data integrity provided by the backup plan.

Risks may be addressed by assessing the individual components in the network, the dependence on each component, and the probability of it going down or

becoming unavailable or unreliable. A financial institution must analyze the business impact- including cost or lost dollars - regulatory and legal requirements, and customer satisfaction to assess backup costs. The costs of various backup alternatives must be weighed against the extent of risk protection each provides. This assessment also should address costs associated with testing, since all components of a plan should be tested periodically, including the communications media.

A financial institution should have a file identifying all circuits by circuit number and a matrix outlining their location, priorities and uses. A duplicate of this file should be maintained at a different location in case of any problems.

The backup plan must address the practicality of each component. Selected alternatives must be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. For example, several dial-up lines may not be a practical replacement for a T1 line. The backup plan must recognize availability and lead times required to employ certain components, such as installing additional lines or modems and multiplexers at a backup site. Reliability, flexibility, and compatibility – all components of the original planning process – also must be considered in formulating the backup plan. For example, a modem used for backup may not provide the service required, or a line may satisfactorily transmit voice, but be insufficient in quality and speed for data. Additionally, the telecommunications backup plan must be compatible with other contingency plans in the institution, since it will affect users, data processing, and customers.

Security and the data integrity of alternative components used must be considered in the contingency plan. Switching from fiber optics to wire pair, dedicated to switched, or digital to analog may make the line more susceptible to a wire tap or to line noise, which can result in errors. Using dial-up lines could facilitate access by the public. Alternate equipment selected should be checked to determine if it permits encryption.

The relative importance of the applications processed and the extent to which a financial institution depends on its telecommunications system will determine the degree of backup required. Management should make a careful appraisal of its backup requirements, decide on an effective plan, detail the procedures, and test its effectiveness periodically.

INSURANCE

Insurance is commonly used to guard against loss from risks that cannot be completely prevented. Generally, coverage is acquired for risks with little probability of occurring, but with significant potential for financial loss or other disastrous consequences.